

**Notice of Allowability**

Application No.

10/059,217

Examiner

Longbit Chai

Applicant(s)

HASHIMOTO ET AL.

Art Unit

2131

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 6/14/2006.
2. ☒ The allowed claim(s) is/are 4-9 and 14.
3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some\* c) ☐ None of the:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.


Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 9/14/2004
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date 7/13/2006
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_.

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100  
Part of Paper No./Mail Date 20060718

## **DETAILED ACTION**

### ***Priority***

Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) – (d) is acknowledged.

The application is filed on 1/31/2002 but has a foreign priority application filed on 1/31/2001.

### ***Examiner's Amendment***

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Eckhard H. Kuesters (Reg. No. 28,870) on 7/13/2006.

This application has been amended as follows:

#### **IN THE CLAIMS**

Cancel claims 1 – 3 and 10 – 13.

Replace claim 14 as follows.

Art Unit: 2131

**Claim 14:** A microprocessor internally having a secret key specific to the microprocessor that cannot be read out to an external device, the microprocessor comprising:

a processor core configured to execute a key registration instruction in which a registration request with an address of a distribution key of a program and a program identifier that identifies a program including plaintext instructions and encrypted instructions is issued, and to execute instructions of another program during a key registration based on the registration request, the distribution key being obtained in advance by encrypting an instruction key specific to the program by using a public key corresponding to the ~~the~~ private key, the encrypted instructions being obtained by encrypting instructions by using the instruction key;

an instruction cache memory configured to store a cache line containing a part of instructions of a program in correspondence to a program identifier, and to permit reading of the cache line only when the program identifier stored in correspondence to the cache line coincides with a program identifier received along with a program reading request from the processor core; and

a key management unit configured to, when receiving the registration request with the address of the distribution key and the program identifier, carry out the key registration, wait for a completion of an invalidation of the cache line corresponding to the program identifier included in the registration request, to notify a completion of the key registration to the processor core asynchronously by interruption when the key registration and the invalidation are both completed to enable the program with respect

to the key registration request to be executed, the key registration being carried out by reading out the distribution key from an external memory based on the address thereof sent from the processor core, to decrypt the distribution key by using the secret key to obtain the instruction key, and to register into a key table the instruction key in correspondence to the program identifier sent from the processor core, the invalidation being carried out by invalidating the cache line stored in correspondence to the program identifier on the cache memory when the instruction key corresponding to the program identifier is registered in the key table,

wherein the processor core starts to execute the program with respect to the registration request by using the corresponding instruction key after receiving the notification of the completion of the key registration from the key management unit.

### ***Allowable Subject Matter***

1. Claims 4 – 9 and 14 are allowed.
2. The following is an examiner's statement of reasons for allowance:

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations, as recited in independent claim 14.

The prior arts Hartman in combination with Alexander, fail to teach or suggest a key management unit configured to, when receiving the registration request with the address of the distribution key and the program identifier, carry out the key registration,

Art Unit: 2131

wait for a completion of an invalidation of the cache line corresponding to the program identifier included in the registration request, to notify a completion of the key registration to the processor core asynchronously by interruption when the key registration and the invalidation are both completed to enable the program with respect to the key registration request to be executed (i.e. using a program identifier that identifies a program including plaintext instructions and encrypted instructions is issued, and to execute instructions of another program during a key registration based on the registration request), the key registration being carried out by reading out the distribution key from an external memory based on the address thereof sent from the processor core, to decrypt the distribution key by using the secret key to obtain the instruction key, and to register into a key table the instruction key in correspondence to the program identifier sent from the processor core, the invalidation being carried out by invalidating the cache line stored in correspondence to the program identifier on the cache memory when the instruction key corresponding to the program identifier is registered in the key table.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Art Unit: 2131

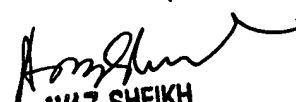
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
LBC

Longbit Chai  
Examiner  
Art Unit 2131

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100